REMARKS

The Specification has been amended. Claims 1 - 3, 7 - 8, 12 - 14, 16, 19, and 21 have been amended, and Claims 4 and 15 have been cancelled from the application without prejudice (and Claim 11 was previously cancelled from the application without prejudice). No new matter has been introduced with these amendments, all of which are supported in the application as originally filed. Claims 1 - 3, 5 - 10, 12 - 14, and 16 - 21 are now in the application.

Applicants are not conceding that the subject matter encompassed by the claims as presented prior to this Amendment is not patentable over the art cited by the Examiner, as claim amendments and cancellations in the present application are directed toward facilitating expeditious prosecution of the application and allowance of the currently-presented claims at an early date. Applicants respectfully reserve the right to pursue claims, including the subject matter encompassed by the claims as presented prior to this Amendment and additional claims, in one or more continuing applications.

I. Rejection under 35 U. S. C. §101

Paragraph 4 of the Office Action dated July 13, 2007 (hereinafter, "the Office Action") states that Claims 16 - 18 are rejected under 35 U. S. C. §101 as being directed to non-statutory subject matter. Independent Claim 16 is amended herein. Accordingly, the Examiner is respectfully requested to withdraw this rejection.

II. Rejection under 35 U. S. C. §103(a)

Paragraph 6 of the Office Action states that Claims 1 - 9 and 11 - 21 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent 7,134,137 B2 to Joshi et al. (hereinafter, "Joshi") in view of U. S. Patent 7,130,885 B2 to Chandra et al. (hereinafter, "Chandra"). Paragraph 7 of the Office Action states that Claim 10 is rejected under 35 U.S.C. §103(a) as being unpatentable over Joshi in view of U. S. Patent 7,131,000 to Bradee. These rejections are respectfully traversed.

Section 706.02(j) of the MPEP, "Contents of a 35 U.S.C. 103 Rejection", states the requirements for establishing a *prima facie* case of obviousness under this statute, noting that three criteria must be met. These criteria are (1) a suggestion or motivation, found either in the references or in the knowledge generally available, to modify or combine the references; (2) a reasonable expectation of success; and (3) the combination must teach all the claim limitations. The three requirements for establishing a *prima facie* case of obviousness are also stated in MPEP §2142, "Legal Concept of *Prima Facie* Obviousness", and MPEP §2143, "Basic Requirements of a *Prima Facie* Case of Obviousness". Section 2143.03 of the MPEP, "All Claim Limitations Must Be Taught or Suggested", discusses the *prima facie* case for obviousness and makes reference to ***In re Wilson***, 165 USPQ 494, 496 (C.C.P.A. 1970), which stated "*All words* in a claim must be considered in judging the patentability of that claim against the prior art." (emphasis added)

Applicants respectfully submit that a *prima facie* case of obviousness has not been made out as to their independent Claims 1, 16, or 19, as will now be demonstrated.

Applicants' Claim 1 recites "authenticating the entity with an authentication service in the local security domain" (Claim 1, lines 7 - 8, emphasis added). This "authenticating" in the local security domain is illustrated by reference numbers **503, 504** in **Fig. 5**. See also Block **430** in **Fig. 4**. Another authentication is then performed in each remote security domain. See reference numbers **508, 509** of **Fig. 5**, which illustrate "authenticating the entity with an authentication service in each of the ... remote security domains" (Claim 1, lines 21 - 23, emphasis added). See also Block **480** in **Fig. 4**. The authenticating in the remote security domains uses "located security credentials", which are "previously-stored security credentials" that are located "by the remote trust proxy in ... the remote security domains" (Claim 1, lines 15 - 17, emphasis added). See also Block **460** in **Fig. 4**. The located security credentials are located "using the identification of the entity from the authentication assertion" (Claim 1, lines 15 - 17) that is forwarded (see reference number **506** of **Fig. 5** and Block **450** of **Fig. 4**) to the remote trust proxy "responsive to a successful outcome of the authenticating" in the local security domain (Claim 1, lines 12 - 14).

Applicants respectfully submit that Joshi does not teach, or suggest, this claimed cross-domain authentication (Claim 1, lines 1 - 2) approach.

With reference to the "authenticating" claim element on lines 7 - 11 of Claim 1, the Office Action cites col. 7, lines 15 - 21 and col. 8, lines 46 - 58 of Joshi. These cited portions of Joshi will now be discussed.

Referring first to col. 8, lines 46 - 58, this text discusses policies and profiles, and "In one implementation, ... administer[ing such information] through delegable Administration roles. Certain users are assigned to [these] Administration roles ...". Applicants fail to see any relevance of user roles and user Administrators to the claim element recited on lines 7 - 11 of Claim 1.

Referring next to col. 7, lines 17 - 27, Applicants respectfully note that this text describes a centralized authentication approach, in contrast to Applicants' claimed approach of first authenticating the entity in the local security domain (Claim 1, lines 7 - 11) and then authenticating the entity in each remote security domain (Claim 1, lines 21 - 28).

Joshi's centralized authentication approach is described, for example, at the following citations:

- col. 5, lines 34 - 39, "... the access management portion of the Access System ... provides security for resources across one or more web servers";
- col. 5, lines 44 - 47, "A key feature of one embodiment ... is the centralization of the repositories for policies and user identity profiles while decentralizing

their administration. That is, one embodiment ... centralizes the policy and identity repositories ..." (emphasis added);

- col. 7, lines 15 - 21, "... Access Server **34** provides authentication ... It further provides for identity profiles to be used across multiple domains and Web Servers from a single web-based authentication ..." (emphasis added);
- col. 7, lines 24 - 27, "Access Server **34** is able to provide centralized authentication ... for resources hosted on or available to Web Server **18** and other Web Servers" (emphasis added);
- col. 17, lines 39 - 41, "Policy domain cache **566** caches all default authentication rules of each policy domain ..." (emphasis added); and
- col. 41, lines 7 - 25, discussing a scenario for "automated login for a downstream application", where the authentication is performed using "user identity profile information" that is apparently centrally-stored, as indicated by lines 15 - 19, stating that the "user identity profile is passed to a downstream application ..." (emphasis added). Lines 12 - 14 also state that the downstream application can use the passed information to authorize (notably, not authenticate) the user, indicating that the *authentication* occurs prior to involvement of this downstream application. See also **Fig.** 47, showing how the downstream application uses the passed data (provided in header variables), which notably omits any reference to performing authentication.

As discussed above, Applicants' Claim 1 recites authenticating first in the local domain,

and then authenticating again in each of the remote domains. Accordingly, this is distinct from Joshi's centralized authentication approach.

Joshi also describes a redirection approach that ensures that authentication is performed at a centralized location by redirecting authentication requests to a server characterized as a "master domain" server. See the following citations:

- col. 30, lines 17 - 23, "... In such a multiple domain case, each of the associated portal Web Servers use a Web Gate plug-in configured to redirect user authentication exchanges to the e-business host's designated web log-in Web Server.". See also col. 30, lines 30 - 32, "As a result, the user is transparently authenticated [by the authentication at the log-in Web server] in both the original associated portal's domain and the e-business host's domain." (emphasis added);
- col. 31, lines 12 - 16, "All resource requests made to any of the multiple protected domains ... are redirected to the preferred host domain, thus requiring the user to authenticate according to the preferred host domain's policy and/or policies. As a result, after authentication at the preferred host domain, the user is transparently authenticated for all other domains residing on the same web server." (emphasis added);
- col. 31, lines 32- 37 describe a scenario involving "a plurality of Web Servers, each hosting a different domain" and stating "... when multiple domains are protected and distributed across multiple Web Servers, the administrator will

identify exactly one of the domains as a 'master domain'." (emphasis added);

- col. 31, lines 43 - 49, "... if authentication handler **512** determines that the domain of the requested resource is a master domain ... then authentication event handler **512** attempts to authenticate at the master domain ... Otherwise, redirection event handler **504** redirects browser **12** to the master domain ... The user then authenticates at the master domain ..." (emphasis added; see also reference numbers **1032 - 1038** of **Fig. 28**);
- col. 31, lines 49 - 55, describing the flows shown in **Fig. 29** where a user's request **1084** at Web Browser **1082** is redirected from Web Server "B.com" to the master domain at Web Server "A.com" for authentication, as shown by flow **1086**; and
- See also col. 32, lines 1 - 3, stating "Any subsequent authentication ... at domain C.com [in **Fig. 29**, where "C.com" is another non-master-domain server] ... follows the [redirection] method of FIG. 28" (emphasis added).

Applicants' Claim 1 does not use this redirection approach of Joshi, which enforces a centralized authentication approach of authenticating at the "master domain". Instead, as discussed above, Applicants' Claim 1 recites authenticating first in the local domain, and then authenticating again in each of the remote domains. Accordingly, this is distinct from Joshi's redirection approach.

Col. 22, lines 33 - 53 of Joshi describe a scenario where a user may be authenticated

twice. The second authentication is not performed (i.e., "The user will be allowed access to the second resource without re-authenticating") in some cases. In particular, the second authentication is not performed "if the authentication level of the authentication scheme used to successfully authenticate [the user] for the first resource is equal to or greater than the authentication level of the authentication scheme of the second resource." (emphasis added).

By contrast, Applicants' claim elements as recited in Claim 1 do not use this "equal to or greater than" test, and do not specify that "The user will be allowed to access the second resource [according to such test] without re-authenticating".

Col. 48, lines 44 - 59 of Joshi describe an embodiment where "affiliate" Web Gates are "installed on remote Web Servers to provide single sign-on authentication across multiple organizations.". However, in contrast to Applicants' claimed approach, ".. the affiliate Web Gate [at the "second company"; see col. 48, lines 53 - 54] will request a Web Gate of the Access System [at the "first company"] to authenticate the customer [from the second company]" (col. 48, lines 56 - 57) for accessing the "subset of resources on the first company's web site" (col. 48, lines 52 - 53).

This redirecting of authentication of a customer at the second site to the Web Gate at the first company is distinct from Applicants' claimed approach as claimed in Claim 1 where an authenticating occurs first at the local security domain (Claim 1, lines 7 - 11); previously-stored credentials are located using information that is forwarded responsive to this

authenticating (Claim 1, lines 15 - 20); and an authenticating then occurs at the remote domain, using the located credentials (Claim 1, lines 21 - 28).

Accordingly, it can be seen that Joshi does not teach all limitations, including all of the words, of Applicants' Claim 1. Applicants respectfully submit that Chandra also fails to teach the limitations not taught by Joshi, as Applicants find no teaching, or suggestion, in Chandra of the above-described "authenticating" (Claim 1, lines 7 - 11), "using the identification ... by the remote trust proxy ... to locate previously-stored security credentials" (Claim 1, lines 15 - 20), and "authenticating" (Claim 1, lines 21 - 28).

Applicants' Claim 1 also recites, in lines 17 - 20, "wherein the located security credentials ... in at least one of the selected remote security domains differ from the security credentials of the entity provided to the initial point of contact" (emphasis added). Applicants find no teaching, or suggestion, in Joshi or Chandra of security credentials that differ, for the (same) entity, among the local and remote security domains in this manner (or of an authentication approach that deals with such differences in the manner claimed by Applicants).

Because the references fail to teach these above-discussed claim limitations, Applicants respectfully submit that (at least) requirement (3) of the *prima facie* case of obviousness ("the combination must teach all the claim limitations"), as noted in the above-cited Sections 706.02(j), 2142, and 2143 of the MPEP, has not been met with regard to Claim 1. Accordingly, independent Claim 1 is deemed patentable over Joshi and Chandra.

Independent Claim 16 recites "initially authenticating ... in a local security domain ..." (Claim 16, lines 6 - 8), "mapping the provided identity, in each of at least one remote security domains, to the different identity requirements ..." (Claim 16, lines 9 - 13), and "subsequently authenticating the entity ... in each of the at least one remote security domains ..." (Claim 16, lines 14 - 17). Independent Claim 19 recites "authenticating the using identity ... in the first security domain" (Claim 19, lines 9 - 10), "using ... the conveyed initial identity information to locate previously-stored identity information ..." (Claim 19, lines 15 - 17), and "using the located identity information, in each of the remote security domains, to authenticate the using entity ..." (Claim 19, lines 18 - 23). Claims 16 and 19 are therefore deemed patentable over Joshi and Chandra according to the same arguments presented above with regard to the "authenticating", "using the identification", and "authenticating" elements on lines 7 - 11, 15 - 20, and 21 - 28 of Claim 1, respectively.

Dependent Claims 2 - 3, 5 - 10, 12 - 14, 17 - 18, and 20 - 21 are deemed patentable by virtue of (at least) the patentability of the independent claims from which they depend. The Examiner is therefore respectfully requested to withdraw the §103 rejection of all claims as currently presented.

III. Conclusion

Applicants respectfully request reconsideration of the pending rejected claims, withdrawal of all presently outstanding rejections, and allowance of all remaining claims at an early date.

Respectfully submitted,

/Marcia L. Doubet/

Marcia L. Doubet
Attorney for Applicants
Reg. No. 40,999

Customer Number for Correspondence: 43168
Phone: 407-343-7586
Fax: 407-343-7587